(19) Europäisch s Pat ntamt
European Pat nt Offic
Offic urop´en d s br vets

(11) EP 0 844 551 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.05.1998 Bulletin 1998/22

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **97890210.4**

(22) Date of filing: **22.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **28.10.1996 US 738897**

(71) Applicant: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(72) Inventor: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(74) Representative: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

Remarks:
A request for correction (exchanging the contents of figure 1 with figure 2 and vice versa) has been filed pursuant to Rule 88 EPC. A decision on the request will be taken during the proceedings before the Examining Division (Guidelines for Examination in the EPO, A-V. 3.).

(54) Computer security system

(57) Several embodiments of computer security systems are described and which are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream. In one embodiment, the security system comprises: an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel, analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to a code; and a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means; and a notification means for receiving said code and for notifying said authorized individual of the identity of said code.

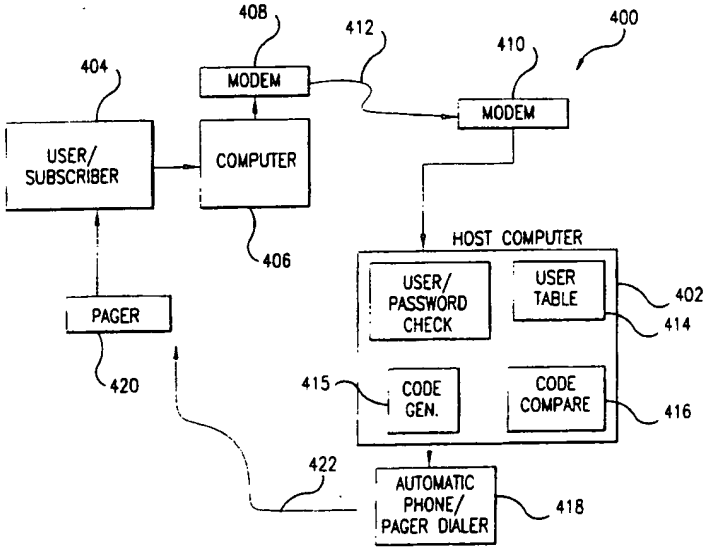


FIG.6

EP 0 844 551 A2

D scription

1. Fi ld of the Inv ntion

The present invention relates to a security and/or access restriction system and, in one embodiment, to a security and/or access restriction system which is adapted to grant only authorized users access to a computer system and/or to certain data which may be resident within the computer system and/or resident within a communications channel and/or other communications medium.

2. Background of the Invention

In recent years, computers have proliferated in all parts of worldwide society, including but not limited to, banking, financial services, business, education, and various governmental entities. For instance and without limitation, these computer systems allow individuals to consummate financial transactions; to exchange confidential scientific and/or medical data, and to exchange highly proprietary business planning data. Hence, these computer systems require and/or allow very sensitive and confidential data to be stored and transmitted over great geographic distances.

Moreover, the rise of multinational communications networks, such as the publicly available Internet communications system, has truly made the world a smaller place by allowing these computers, separated by great geographic distances, to very easily communicate and exchange data. In essence, these worldwide communications channels/networks, sometimes collectively referred to as "the Information Superhighway" have electronically connected the peoples of the world - both the good and the very bad.

That is, while these computer systems have increased efficiency and greatly changed the manner in which we work and interact, they have been especially prone to unauthorized "break-ins", viral destruction, and/or unauthorized data modifications. Accordingly, the rather sensitive and confidential data which is stored and used within these computer systems and transmitted between these computer systems has been the target of attack by people known as "hackers" and by high level and very sophisticated espionage and industrial spies. Computer access security and data transmission security has recently come to the forefront of importance and represents one of the great needs of our times.

Many attempts have been made to create and utilize various techniques (hereinafter the term "technique" as used and/or employed in this Application refers to any combination of software, hardware, and/or firmware which comprise an apparatus and a methodology whose components cooperatively achieve an overall security objective) to "ensure" that only authorized users are allowed to gain access to these respective computer systems. These prior techniques, while somewhat effective, suffer from various drawbacks.

For example, one such prior computer system security technique comprises the use of predetermined "passwords". That is, according to this security technique, each computer system has a list of authorized passwords which must be communicated to it before access is given or allowed. In theory, one or more "trusted" system administrators distribute these "secret" passwords to a group of authorized users of a computer system. The "secret" nature of the passwords, in theory, prevents unauthorized users from accessing the computer system (since presumably these unauthorized users do not have the correct passwords). This technique is not very effective since oftentimes those authorized individuals mistakenly and unwittingly expose their password to an unauthorized user Moreover, this technique of data security may be easily "broken" by a "hacker's" deliberate and concentrated attempt at automatically inputting, to the targeted computer, hundreds and perhaps thousands of passwords until an authorized password is created.

In addition to the prior password technique other, more sophisticated access techniques are known and used. For example, there are known techniques which require the possession of a physical object or feature, such as "access cards" which are "read" by a card reading device and biometric authentication techniques (e. g. requiring the initial input of such authorized user physical characteristics as fingerprints and eye patterns and the later comparison of these input patterns to those of a "would-be" user). Both of these prior techniques are relatively complicated, are relatively costly, and are prone to error, such as and without limitation, mistaken unauthorized entry due to their complexity. These techniques are also prone to unauthorized entry by use of counterfeit and/or stolen cards, objects, and fingerprint readers. Other prior data security techniques, such as encryption, attempt to prevent unauthorized use of transmitted data or unauthorized access to a computer system by modifying and/or changing the transmitted data in a certain manner, and/or requiring the transmission and receipt of modified data before access is granted. While somewhat effective, these prior encryption techniques are relatively costly and complicated and require one or more known "encryption keys" which are in constant exchange between users and which are themselves susceptible to theft and/or inadvertent disclosure. Furthermore, the best-known and perhaps strongest encryption algorithm is proprietary and cannot be used without a costly license. Moreover, since the encrypted message still provides all of the transmitted data, in some form, it is still possible for one to gain access to the entire data stream by "breaking the encryption code". Since no encryption algorithm is ever considered "unbreakable", encryption is not considered to be a "foolproof' security solution.

There is therefore a need to provide a technique to substantially prevent the unauthorized access to one or

more computer systems and which overcomes the various drawbacks of these afore-described prior techniques. There is also a need to provide a technique to substantially prevent the unauthorized interception and use of transmitted data and which overcomes the various drawbacks of the prior art. Applicant's invention(s) seek and do meet these needs. Applicant's invention, in one embodiment, achieves these objectives by splitting the data into a plurality of separate communication channels, each of which must be "broken" for the entire data stream to be obtained. In essence, in this embodiment of Applicant's invention, cooperatively form the entire message. The splitting of the data in this manner may also "fool" the would be data thief into believing that he or she has obtained all of the data when, in fact, only several communication channels are obtained.

SUMMARY OF THE INVENTION

While a number of "objects of the invention" are set forth below, it should be realized by one of ordinary skill in the art that the invention(s) are not to be limited, in any manner, by these recited objects. Rather, the recited "objects of the invention" are to be used to place Applicant's various inventions in proper overall perspective and to enable the reader to better understand the manner in which Applicant's inventions are to be made and used, especially in the preferred embodiment of Applicant's invention. Accordingly, the various "objects of the invention" are set forth below:

It is a first object of the present invention to provide a technique to substantially ensure that only authorized users gain access to a computer system.

It is a second object of the invention to provide a technique to substantially ensure that only authorized users gain access to a computer system and which overcomes the various previously delineated drawbacks of the prior computer system security techniques.

It is a third object of the invention to provide a technique to substantially ensure that only authorized users have access and use of certain transmitted data appearing, for example, within a data stream.

It is a fourth object of the invention to provide a technique to substantially ensure that only authorized users have access and use of certain transmitted data and/or certain hardware, software, and/or firmware which cooperatively form and/or comprise a computer system, and that this technique overcomes the various previously delineated drawbacks of the prior techniques.

According to a first aspect of the present invention, a security system is provided. Particularly, the security system is adapted to be used in combination with a computer and to only grant an authorized individual access to the computer. The security system comprises, in one embodiment, password means for receiving a password by use of a first communications channel; and code generation means, coupled to said password means, for generating a code by use of a second communications channel, and to allow that individual access to the computer system only if that individual generates and communicates the code to the code generation means.

According to a third aspect of the present invention, a method is provided for use with a computer and effective to substantially prevent an unauthorized user from accessing the computer. The method comprises, in one embodiment, the steps of assigning a password to the user; receiving the password by use of a first communications channel; generating a code in response to the received password; transmitting the code by use of a second communications channel to the user; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer.

According to a fourth aspect of the present invention, a security system is provided to grant an authorized individual access to a secured stream of data bits. In one embodiment, the data security system comprises a data stream dividing means for receiving said stream of data bits and dividing said stream of data bits into a plurality of sub-streams; transmitting means for transmitting said sub-streams in a predetermined order over a communication channel; and a decoding means for receiving said sub-streams and for recombining said received sub-streams to create said secured stream of data bits.

Further objects, features, and advantages of the present invention will become apparent from a consideration of the following description, the appended claims, and/or the appended drawings. It should further be realized by one of ordinary skill in the art that the previously delineated objects and aspects of the invention are for illustration purposes only and are not to be construed so as to limit the generality of the inventions and/or to limit the interpretation to be given to the various appended claims. Moreover, it should also be realized by those of ordinary skill in the art that the term "communications channel" as used throughout this Application refers to any physical and/or electromagnetic means or method of transferring and/or communicating information from one or more sources to one or more receivers. Moreover, the term "communications channel" should be given the broadest known interpretation covering any method and/or medium which facilitates the transfer of information and/or over which such information is transferred.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller and more complete understanding of the nature and objects of the present invention, reference should be had to the following drawings wherein:

FIG. 1 is a block diagram of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred security techniques of the invention:

FIG. 2 is a block diagram of another embodiment of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention:

FIG. 3 is a block diagram of yet another embodiment of a security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention:

FIG. 4 is a block diagram of another embodiment of a computer security system made in accordance with the teachings of the preferred embodiment having the preferred techniques of the invention:

FIG. 5 is a schematic diagram of a password table used by the computer security systems shown in Figures 1 and 2: and

FIG. 6 is a block diagram of one embodiment of the preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to Figure 1, there is shown a block diagram of a computer security system 10, made in accordance with the principles of the preferred embodiment of the invention and adapted for use in combination with computer 80. More particularly, computer security system 10 selectively allows communication and/or data processing access to computer 80 in a manner which is technically described throughout the remainder of this Application. As shown, security system 10 includes an "analyzing means" 12 and a "random code generating means" 14.

In one embodiment of the preferred embodiment of the invention, analyzing means 12 comprises one or more software subroutines which are adapted to execute upon and/or within computer 80. Alternatively, analyzing means 12 may comprise a microprocessor and/or similar type of computer which is adapted to operate under stored program control in the manner set forth in this Application. One example of another type of computer operating under stored program control and which may be used by the preferred embodiment of the invention is shown and described within chapter eight of the text entitled Advanced Computer Architecture: Parallelism Scalability, Programmability, which was authored by Kai Hwang, which is published by McGraw-Hill, Inc., which has a library reference number of ISBN 0-07-031622-8, and the entire text of all of the chapters of which are fully and completely incorporated herein by reference, word for word and paragraph for paragraph. In either embodiment, analyzing means 12 receives and compares at least two "sets" or streams of data. Should the individually received "sets" match, analyzing means 12 generates and communicates an "access granted" command to computer 80, allowing individual 18 access to the computer 80 Moreover, random code generating means 14 may similarly comprise a conventional pseudo-random number generator which may be constructed or developed on one or more software subroutines which reside and operate/execute upon and/or within computer 80 or may comprise a microprocessor and/or similar type of computer which operates under stored program control.

In operation, individual 18, desiring access to and within computer 80 utilizes a first communication channel 82 (e.g. a first telephone line, radio channel, and/or satellite channel) and communicates, by use of his or her voice or by use of a computer 19 a first password to analyzing means 12. Analyzing means 12 then checks and/or compares this first received password with a master password list which contains all of the authorized passwords associated with authorized entry and/or access to computer 80.

As shown in Figure 5, in the preferred embodiment of the invention, analyzing means 12 contains a master password list 200 having a first column of entries corresponding to authorized passwords necessary to gain access to computer 80. Moreover, as further shown in Figure 5, each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user.

If the received password matches an entry of the master password list, analyzing means 12 generates a command, by means of connecting bus 17 or software message or function call to random code generating means 14 and causes the random code generation means 14 to generate a substantially random and/or pseudo-random number or code, of programmable length, and to transmit the number and/or code, by means of a second communications channel 84, to the individual 85 associated with the received password 202 in the master password list. That is, as should be apparent to one of ordinary skill in the art, code generation means 14 includes both a random number generator and a conventional and commercially available communications interface (e.g. modem and/or telephone/pager interface), allowing the generated pseudo-random code to be generated or communicated over a wide variety of mediums.

Further, it should be apparent that individual 85 may or may not be the same person as individual 18 . If individual 18 was the individual identified in the master password list (e.g. "was authorized"), that individual 18 receives the pseudo-random number and transmits the number to the analyzing means 12, by means of communications channel 82. Once the pseudo-random number is received by the analyzing means 12, from channel 82, it is compared with the number generated by generation means 14. If the two codes are substantially the same, entry to computer 80 and/or to a certain part of computer 80 such as, without limitation, the hardware, software, and/or firmware portions of computer 80 is granted to individual 18. For instance, in another em-

bodiment, table 200 of Figure 5 could contain yet another set of entries specifying the directories or portions of computer 80 that the individual 18 was allowed to have access to. In this manner, allowed access to computer 80 would be further restricted to those computer portions which are specified within table 200. It should be apparent to one of ordinary skill in the art that these portions may be different for different users and that each authorized user may have a different portion that may be accessed in an authorized manner.

It should be apparent to one of ordinary skill in the art that Applicant's foregoing computer security technique is a relatively low-cost, but effective technique, for properly ensuring that only authorized users gain access to a computer system, such as computer system 80. That is, Applicant's foregoing computer security embodiment, utilizes two distinct communications channels and a random number generator in order to ensure that an authorized user of a computer system is notified that someone or something is seeking access to the computer system with his or her password. Moreover, Applicant's foregoing invention is very cost effective as it employs substantially "off the shelf' and readily available components. Further, the use of a "secret" password, a "secret" substantially random number, and a "secret" second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art.

Referring now to Figure 6 there is shown a computer system 400 made in accordance with the teachings of the preferred embodiment of the invention and representing one example and/or implementation which is made in accordance with the various teachings of the preferred embodiment of the invention As shown, computer system 400 includes a host computer 402 (corresponding to computer 80 of the system shown in Figure 1) to which a user or other individual 404 (corresponding to individual 18 of Figure 1) desires access to. As further shown in Figure 6. As shown, individual 404, in this implementation example, utilizes a commercially available and conventional computer 406 and a commercially available and conventional modem 408 to communicate with a commercially available and conventional modem 410 by means of a typical communications channel (e. g. a conventional "dial-up" telephone line) 412. Hence, the user 404, in this embodiment, only requires conventional computer equipment. Host computer 402, in this embodiment, requires a conventional and commercially available automatic dialer which is altered, in a known manner, to receive and pass one or more passwords and/or codes as data.

In operation, user 404 dials through and/or by means of his or her computer 406 and modem 408 in the usual and conventional manner to connect and access host computer 402. The host computer 402, using the principles of the preferred embodiment of this invention, answers the requester's call, which occurs over channel 412, and requests and receives the user's identification code. host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402. This comparison, is a match is made, causes the "code generator" software subroutine 415, resident within computer 402, to generate a pseudo-random number code and passes the received code along with the authorized user's pager number to the commercially available and conventional automatic dialer 418. The automatic dialer 418 telephones the conventional and commercially available pager 420 by means of conventional and commercially available communication channel 422 (e.g. voice line) and transmits the code to the user's pager. As this happens, the host computer 402 awaits the reply from the user attempting to gain access to the computer.

The user 404 now enters the code he or she has received from the pager 420 and any timing instructions which, in yet another embodiment of the invention may also be transmitted from computer 402, and sends this password or pseudo-random code back to computer 402 where it is compared within the software subroutine module denoted as "code compare" 416 in Figure 6. If the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.

Referring now to Figure 2, there is shown a second embodiment of a computer security system made in accordance with the teachings of the preferred embodiment of the invention. This second embodiment 20 is substantially similar to system 10 but also includes a timer or "timing means" 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80 or may comprise a microprocessor which operates under stored program control. In one embodiment, timing means 40 comprises a conventional "watchdog timer" as will be apparent to those of ordinary skill in the art.

In operation, timing means 40 records the time at which the first and second passwords are received by analyzing means 12. Timing means 40, in one embodiment which is coupled to analyzing means 12 and code generation means 14 by bus 42 and in another embodiment which is in software communication with means 12 and 14, then compares the times to determine whether the second password was received within a predetermined period or predetermined "window" of time after the first password was received. In the preferred embodiment of the invention, the predetermined period of time is programmable. The predetermined period of time, will typically need to vary according to the nature or the communications medium used by means 14 to notify individual 85 of the value of the generated code. For example, the predetermined period of time would be shorter when communications channel 84 comprises a pager or cellular phone, since the owner has immediate access to the code upon transmission: and longer

when communications channel 84 comprises a voice-mail system which the owner has to affirmatively access to receive the code. If the second password was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g. computer 80). If the second password was received within the predetermined period of time, analyzing means 12 compares it to the code which was previously generated. If the second password is not substantially identical to the previously generated code, analyzing means 12 denies individual 18 entry to the secured domain (e.g. computer 80). If the received password is substantially identical to the code, analyzing means 12 grants individual 18 entry into the secured domain. As will be readily apparent to those of ordinary skill in the art, timing means 40 provides yet a third level of security to computer system 80. Moreover, it should also be apparent to one of ordinary skill in the art that this "predetermined time" may be as short or as small as several milli-seconds or micro-seconds. This is particularly true if, in yet another embodiment of Applicant's invention, the password generated by communication means 14 is received by a computerized device which is adapted to received the password and to generate a new password code in a substantially automatic manner.

Referring now to Figure 3, there is shown a block diagram of a third embodiment of a computer security system made in accordance with the principles of the preferred embodiment of the invention As shown, computer security system 70 is adapted to receive an input data stream 72, comprising in a first embodiment, a plurality of digital data bits 73, which are to be securely transmitted to a distant site. System 70, as further shown, includes a data stream dividing means 74 which in one embodiment comprises a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of received data and places, in a certain predetermined manner (e.g. alternately) some of the received data bits onto the first communications channel 76 and some of the received data bits onto the second communications channel 78. In this manner, one attempting to wrongfully intercept and/or access the data stream 72 would need access to both communications channels 76, 78 and would need to know the dividing algorithm that dividing means 74 utilizes to divide the received data for placement onto channels 76,78. Applicant's third embodiment therefore provides a very high level of data transmission security.

As further shown in Figure 3, in this third embodiment of the invention, security system 70 further includes a decoding means 88 which may comprise a commercially available microprocessor operating under stored algorithmic program control and which contains "mirror image" of the algorithm used to divide the data stream transmitted to it by means 74. In this manner, the data from each of the channels 76,78 is reconstituted onto single channel 89, in substantially the exact same manner that it was received by means 74. In essence, this third embodiment of Applicant's invention allows and/or provides for the "splitting" of a data stream into a plurality of channels in a predetermined manner and the concomitant reconstitution of the data stream once the data has traversed the communications medium. Hence, the embodiment in Figure 3 splits the data stream so that anyone getting access to one of the channels 76, 78 can't reconstruct the data stream because they're missing half or more of the information. If more channels are used, each channel carries far less than one-half the information.

Referring now to Figure 4 there is shown a fourth embodiment of a computer security and/or data transmission system 100 which is made in accordance with the teachings of the preferred embodiment of the invention As shown, system 100 is adapted to receive a plurality of data bits 103 contained in a first communications channel 102. It should be noted that the data contained within this channel 102 is interspersed with a plurality of "non-data" or filler data bits or "material" 104 according to some predetermined and/or randomly varying algorithm (e.g. every third bit space is filler data) by a microprocessor system 106 which is operating under stored program control. The filler data 104 is binary data and cannot be deciphered as "filler" by an unauthorized user. Therefore, even if one were to intercept the transmitted data, one could not decipher or decode the data. System 100 further includes a decoder 110 for the data reception and decodes 202 for the algorithm reception which, in one embodiment, comprises a microprocessor acting under stored program control and which is adapted to "strip off" the "filler" bits and to allow the originally transmitted data to be reconstituted. In this manner, data may be safely transmitted and received in an authorized manner. In yet another embodiment of the invention which is shown in Figure 4, the algorithm which controls the filler pattern and/or the way that the filler data is interspersed within the "regular" data pattern may be periodically changed in a known and predetermined manner. In this embodiment, the filler data is interspersed within the "regular" data according to a varying filler algorithm (e.g. every three bits for the first 99 bits and then every four bits thereafter). In this embodiment, decoder 110 is adapted to "strip" off these filler bits by having prior knowledge (e.g. embedded within a computer program resident within and controlling the decoder) of the varying algorithms which are utilized by system 100. Here, in the embodiment shown in Figure 4, unlike that shown and described with respect to Figure 3, all the data is transmitted on a single channel but is "muddied."

In yet another embodiment of the invention, as shown in Figure 4, a varying data key is transmitted to decoder 110 and/or decoder 202 by microprocessor system 106 by use of a second channel 200. In this manner, a second channel is needed to tell or communicate the manner in which the filler data is interspersed within the regular data so that the decoder 110 may "strip off" the filler data. In this manner, the filler patterns may be

dynamically changed. Hence, this system utilizes dual/multi channel media to communicate the cryptic modulation of the data with filler.

It is to be understood that the invention is not limited to the exact construction or method illustrated and described above, but that various changes and modifications may be made without departing from the spirit and scope of the invention as defined in the following claims.

Claims

1. A security system for use in combination with a computer, said security system comprising:

 An analyzing means for receiving first password, for generating a first signal in response to said received first password, for receiving a first code, for receiving a second code, and for allowing access to said computer only if said first and said second codes are substantially identical and:
 code generation means for receiving said first signal and for generating and communicating said first code to said analyzing means.

2. A method to restrict access to a certain group of individuals to a computer, said method comprising the steps of:

 assigning a unique password to each of said certain group of individuals:
 assigning a telephone number to each of said unique passwords:
 receiving a data stream:
 comparing said data stream to each of said unique passwords identifying one of said unique passwords with said data stream:
 generating and transmitting a first code to said telephone number associated with said one identified password:
 receiving a second code:
 comparing said first and said second codes; and
 allowing access to said computer only is said first and said second codes are substantially identical.

3. A method to securely transmit data comprising the steps of:

 receiving said data:
 distributing said received data into a plurality of communications channels:
 transmitting said distributed data by use of said plurality of communication channels:
 receiving said distributed data:
 and reconstituting said data.

4. A method to securely transmit data having a plurality of bits, said method comprising the steps of:

 interspersing a plurality of filler data bits into said data in a certain pattern:
 transmitting said data and aid interspersed filler data:
 receiving said data and said interspersed filler data:
 and discarding said interspersed filler data.

5. A security system adapted to grant an authorized individual access to secured domain, comprising:

 an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel. analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to code: and
 a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means.

6. The invention according to claim 1 wherein said analyzing means if further comprises a timing means for recording the time that said first password is received and granting access to said secured domain only if said second password is received within a predetermined period of time.

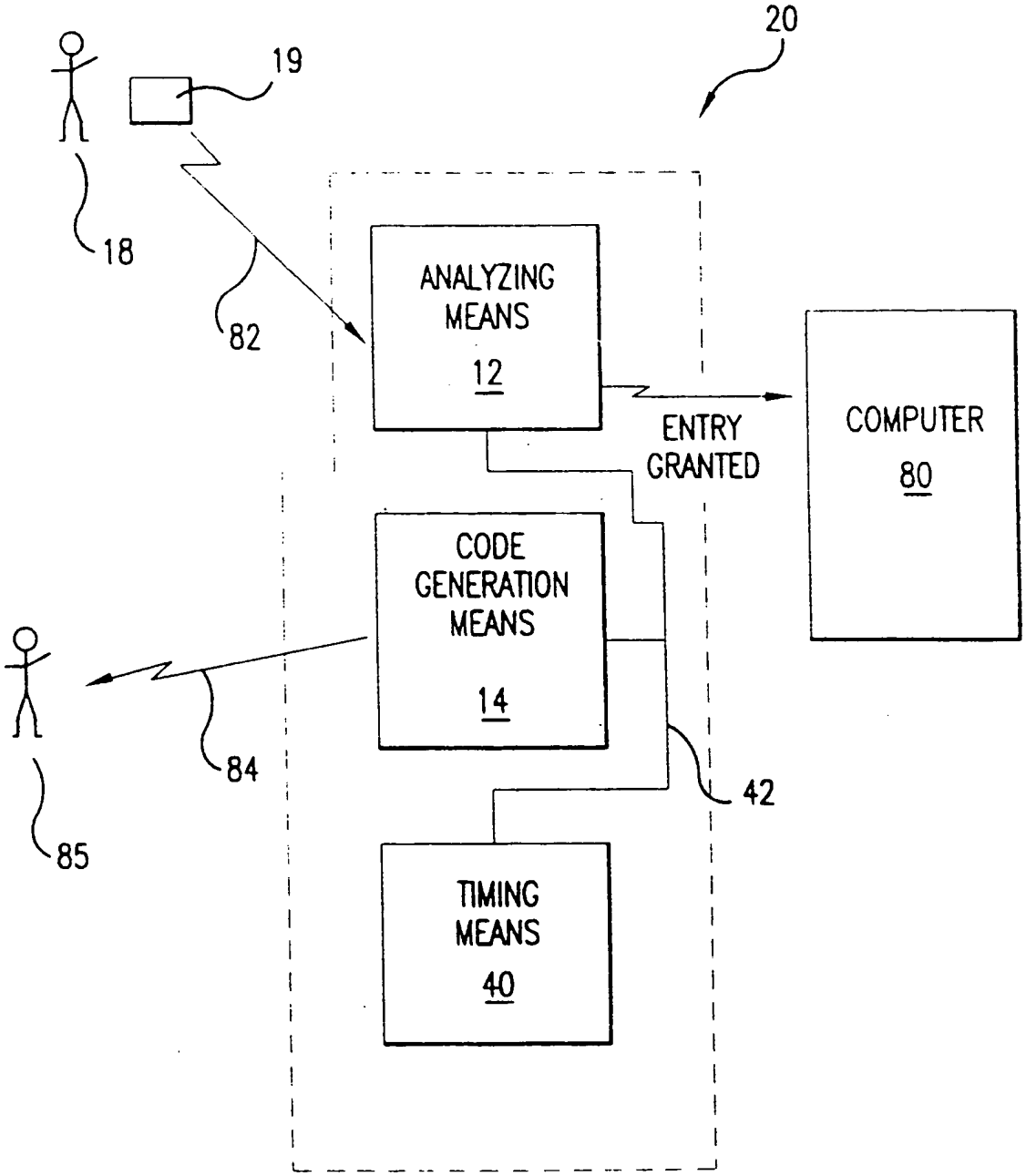

20
19
18
82
ANALYZING MEANS
12
ENTRY GRANTED
COMPUTER
80
CODE GENERATION MEANS
14
84
85
42
TIMING MEANS
40

FIG.1

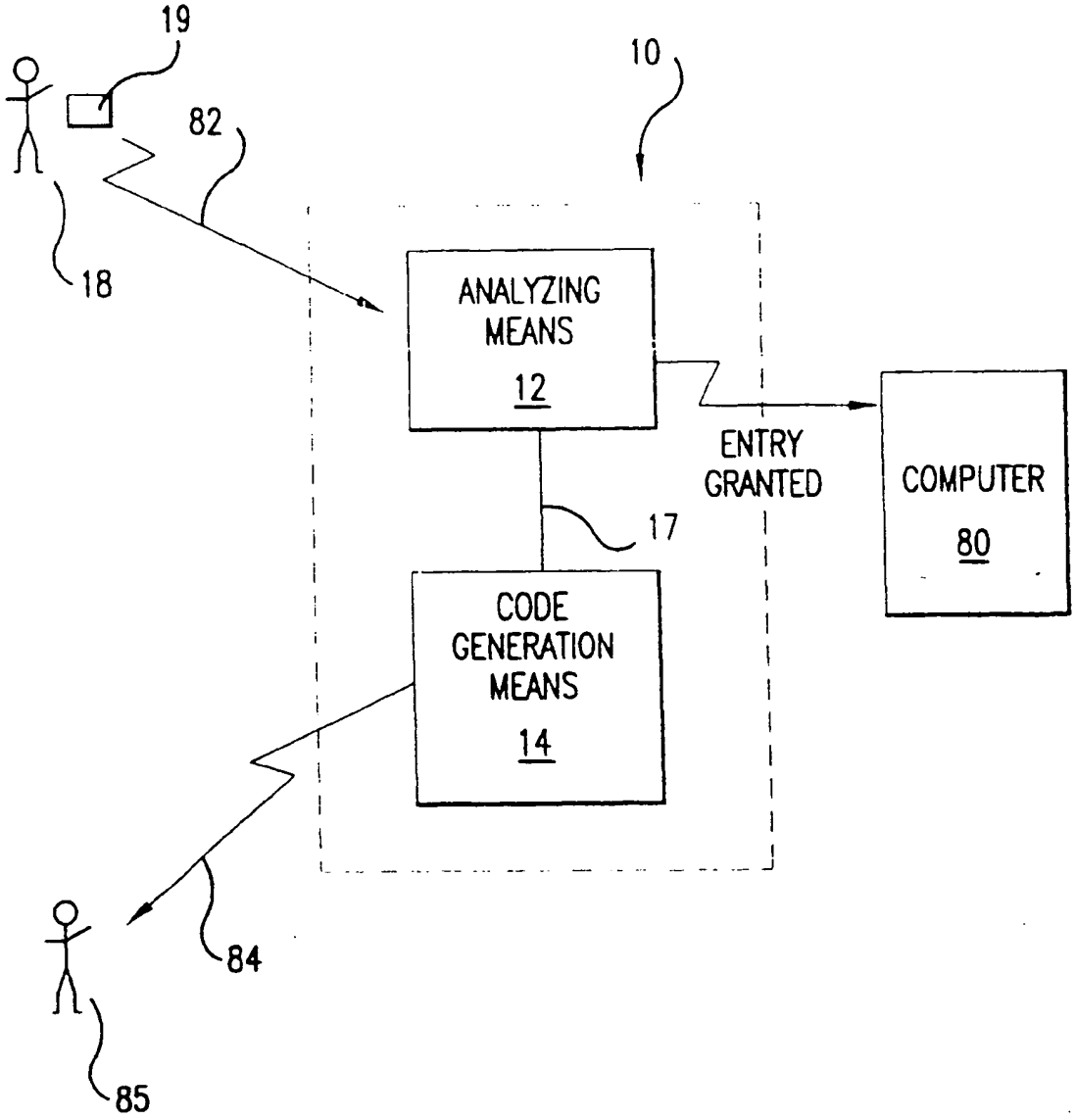

19
10
82
18
ANALYZING MEANS
12
ENTRY GRANTED
COMPUTER
80
17
CODE GENERATION MEANS
14
84
85

FIG.2

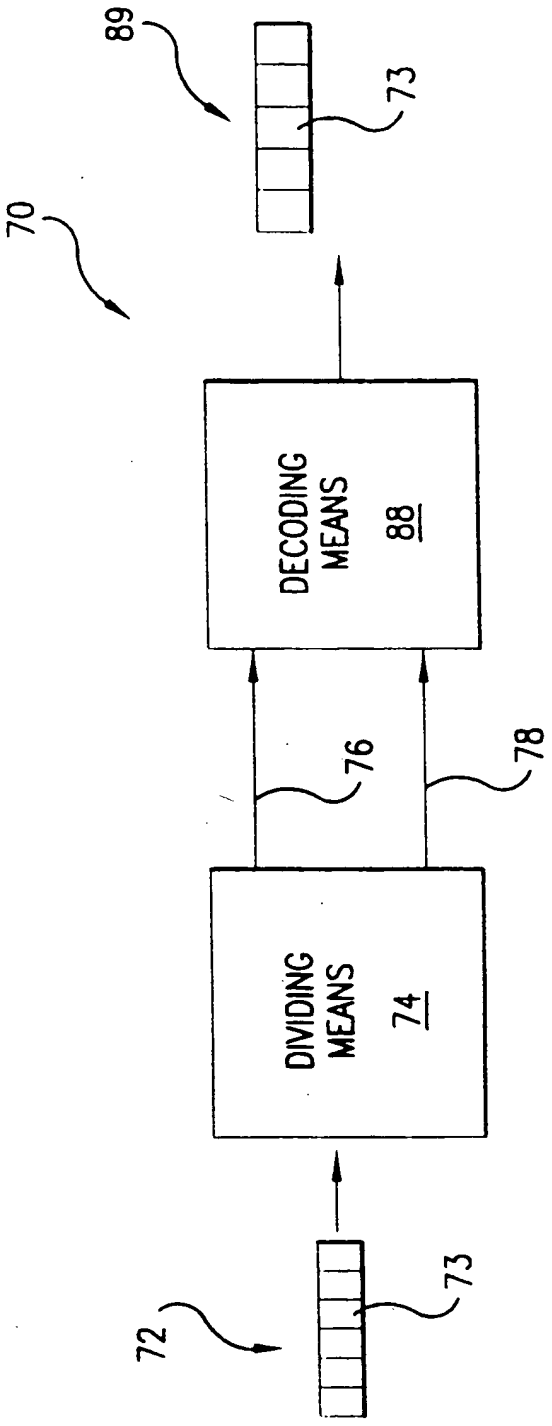


FIG.3

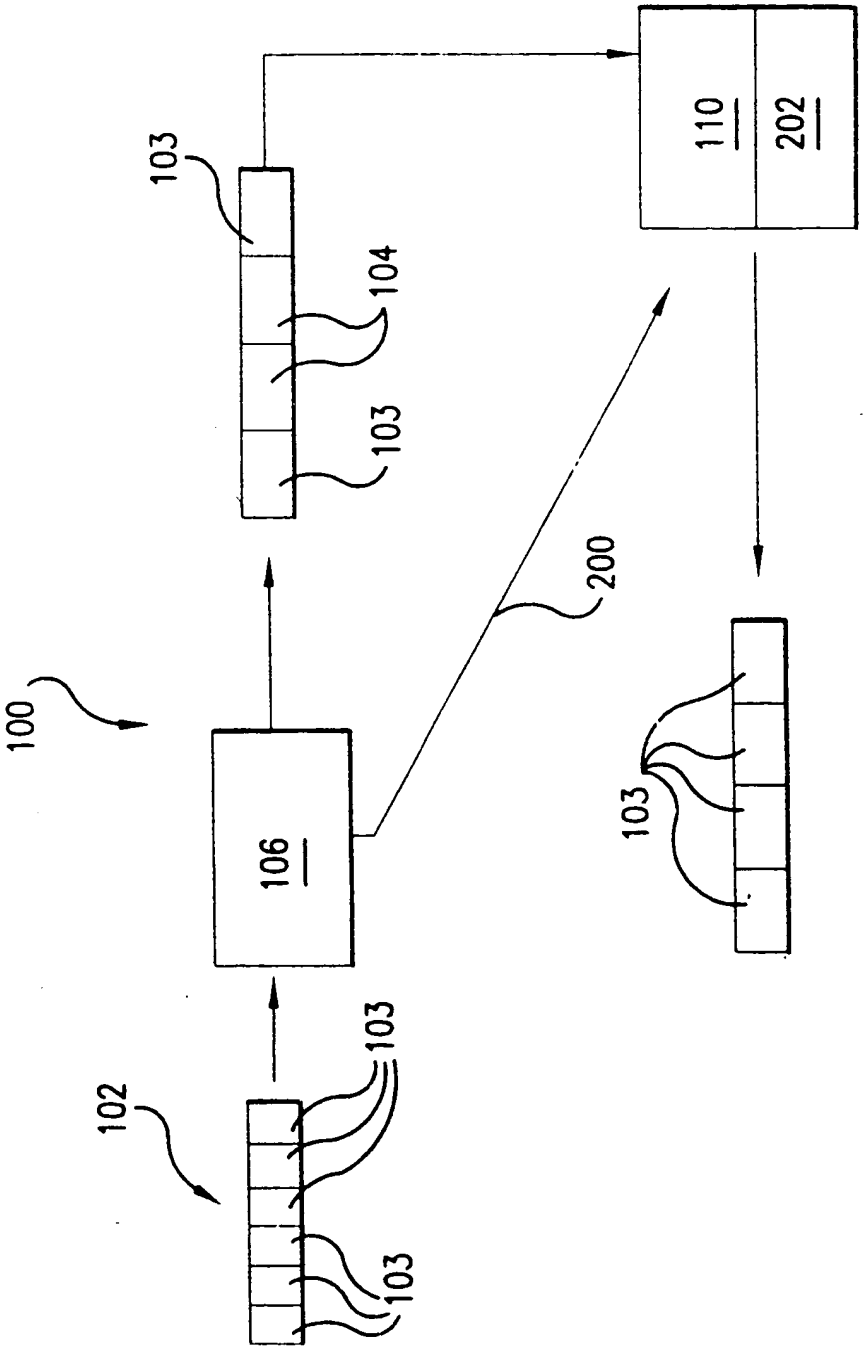


FIG.4

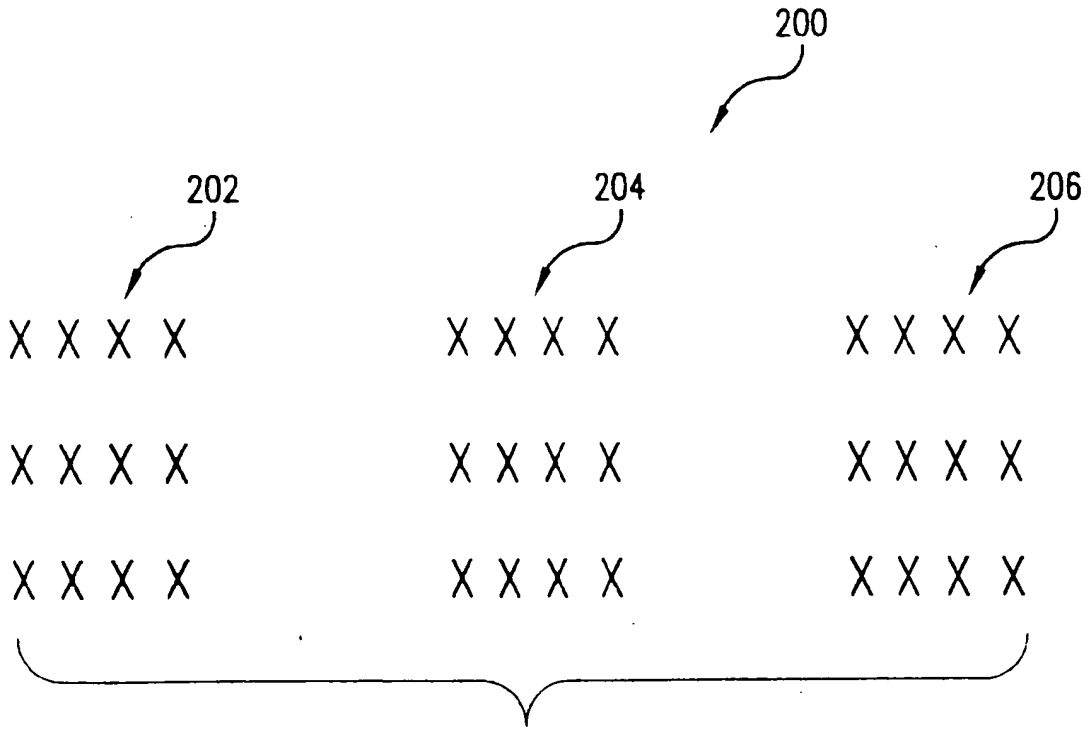


FIG.5

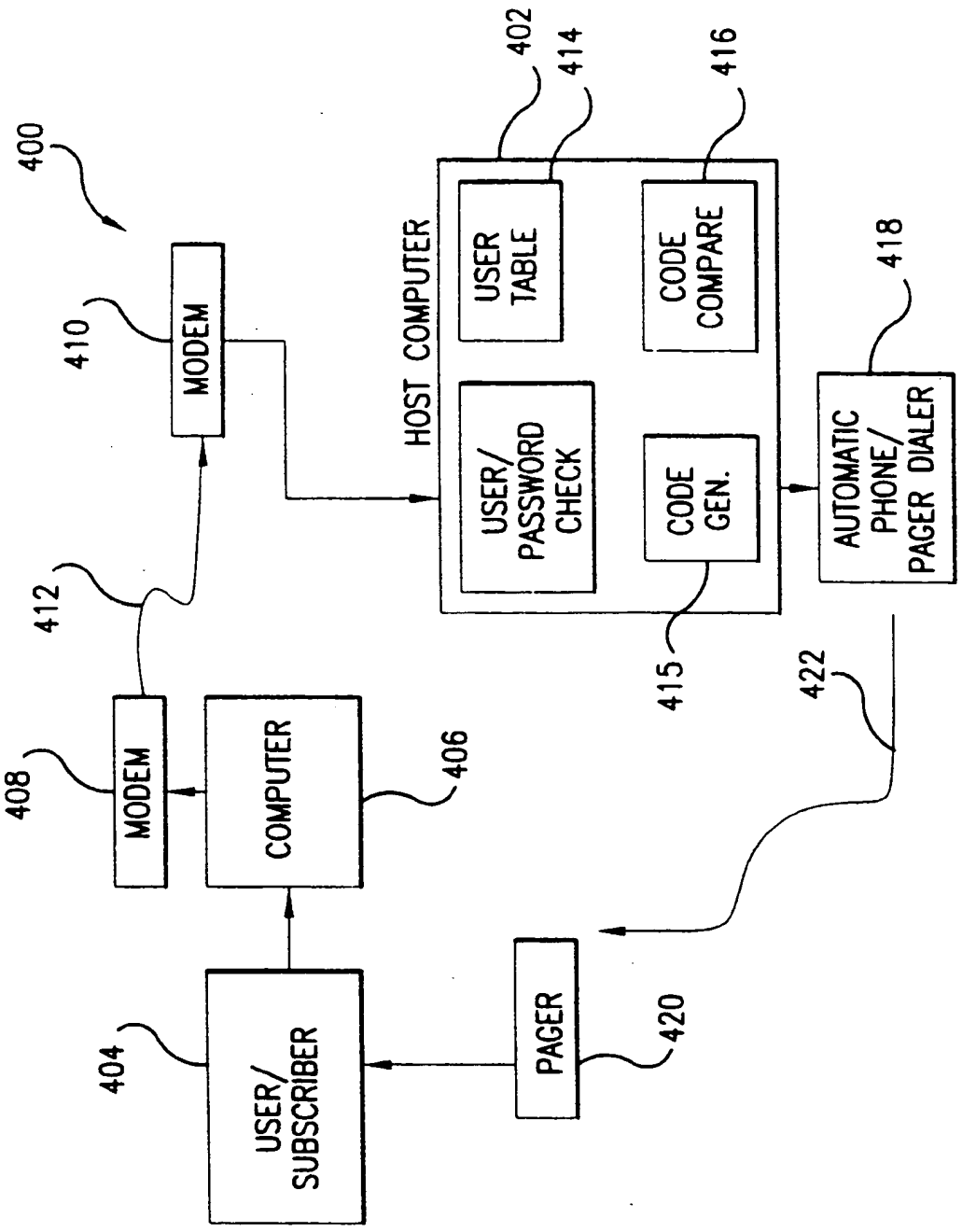

400
402
414
416
410
MODEM
HOST COMPUTER
USER TABLE
CODE COMPARE
418
USER/ PASSWORD CHECK
CODE GEN.
AUTOMATIC PHONE/ PAGER DIALER
412
415
422
408
MODEM
COMPUTER
406
404
USER/ SUBSCRIBER
PAGER
420

FIG.6

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 844 551 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.07.1998 Bulletin 1998/27

(43) Date of publication A2:
27.05.1998 Bulletin 1998/22

(21) Application number: **97890210.4**

(22) Date of filing: **22.10.1997**

(51) Int Cl.[6]: **G06F 1/00**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **28.10.1996 US 738897**

(71) Applicant: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(72) Inventor: **Veneklase, Brian J.**
San Antonio, TX 78249 (US)

(74) Representative: **Matschnig, Franz, Dipl.-Ing.**
Siebensterngasse 54
1070 Wien (AT)

(54) Computer security system

(57) Several embodiments of computer security systems are described and which are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream. In one embodiment, the security system comprises: an analyzing means for receiving first and second passwords, each of said passwords being transmitted over a first communication channel, analyzing said first password, transmitting a first signal output only if said first password is authorized, and granting access to said secured domain only if said second password is substantially identical to a code; and a random code generating means for generating said code, transmitting said code over a second communication channel upon receipt of first signal output, and transmitting said code to said analyzing means; and a notification means for receiving said code and for notifying said authorized individual of the identity of said code.

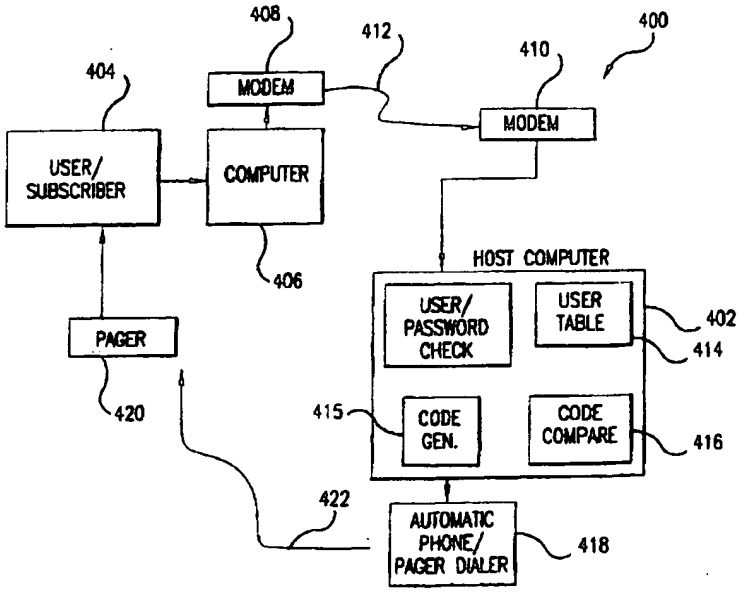


FIG.6

EP 0 844 551 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 89 0210

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 95 19593 A (KEW MICHAEL JEREMY ;LOVE JAMES SIMON (GB)) * abstract; figure 1 * * page 1, line 20 - page 3, line 23 *	1,5	G06F1/00
Y	---	6	
X	GB 2 229 020 A (ELLIS CHRIS KEIRON) * abstract * * page 3, paragraph 2 - page 6, last paragraph * * page 7, paragraph 2 - page 8, paragraph 1 *	2	
Y	---	6	
A	EP 0 558 326 A (HUGHES AIRCRAFT CO) -----		
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			G06F

~~The present search report has been drawn up for all claims.~~

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 February 1998	POWELL D.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& . member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ All claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for all claims.

☐ Only part of the claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid.

namely claims:

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions.

namely:

See Sheet B.

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid.

namely claims:

☒ None of the further search fees has been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims.

namely claims: 1,2,5,6

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 97 89 0210

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1,2,5,6

 Secure access to a computer

2. Claim : 3

 Data transmission using plural channels

3. Claim : 4

 Data transmission with interspersed filler data